

ARIZONA

DEPARTMENT OF ADMINISTRATION
TECHNOLOGY

AD18016
Insider Threat Risk Management
User and Entity Behavior Analytics
April 17, 2019

Background

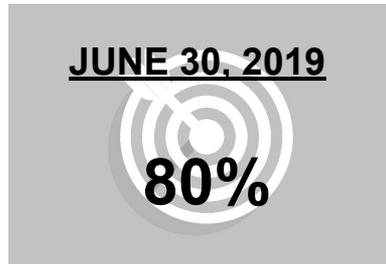
AD18016 - Insider Threat Risk Management

- Cloud Access Security Broker (CASB)
- Phishing
- User and Entity Behavior Analytics (UEBA)

CASB
76.4% Deployed
100% Funds Spent



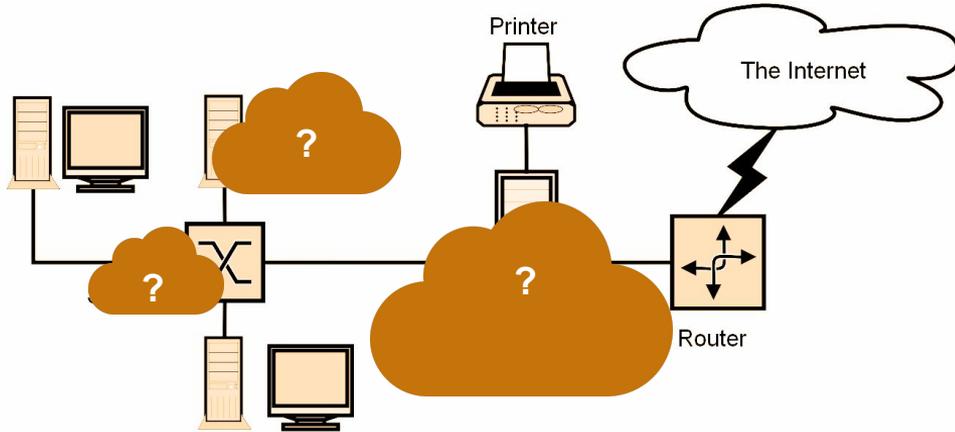
Phishing
65% Deployed
100% Funds Spent



UEBA - What Happened?

Unknown Enterprise Environment

Cost Prohibitive Cloud Consumption Model



input/output

Lessons Learned

- The originally planned architecture was cost prohibitive in the cloud consumption model originally envisioned
 - POC for New Technologies
 - Detailed Specification Reviews

- Variances in milestones and work to be performed under professional services
 - Written vs Verbal SOW
 - Detailed Milestones and Success Criteria

Overall Roll-Out Plan

Planning

- Architecture Design
- Milestones
- Schedule
- SOW
- Success Criteria
- Use Cases

COMPLETE

Approval

- Vendor
- Project Team
- SPO
- ASET
- ESPAC
- ITAC

BY APRIL 17

Install/Configuration

- Hardware
- AA/DL Install
- Use Case Validation

BY MAY 17

Log Ingestion /
Testing

- Logs Sent
- Training by Vendor
- ADOA Testing and Acceptance

BY MAY 24

Deployment

- Deployment
- Invoice Issued

BY JUNE 5

Financials Update

Fiscal Year	FY19	FY20	FY21	FY22	FY23
Development Cost - Licensing	\$1,268,000	\$0	\$0	\$0	\$0
Development Cost - Professional Services	\$132,000	\$0	\$0	\$0	\$0
Operational Cost	\$4,500	\$14,400	\$926,061*	\$14,400*	\$926,061*
Total Cost	\$1,404,500	\$14,400	\$14,400	\$0	\$0

*Depending if product is renewed or some kind of language

Questions??